NP

P { Problems that have poly time algo }

NP = { Problems that has non-deterministic poly time algo }

If yes, we can guess

SAT (satisfiability)

Given (1) variables $x_1, \dots, x_n$

(2) clauses $C_1, \dots, C_m$

$C_i = \{ x_{i_1} \vee \neg x_{i_2} \dots \}$

Find if $\exists$ assignment of $\{T, F\}$ to $\{x_1, \dots, x_n\}$

s.t. all clauses

Obviously, $P \leq NP$

$(a \vee b \vee c)$, $(\neg a \vee \neg b \vee c)$

Question: $P = NP$?

$NP = \{$ problems that admit a poly size certificate (proof) and a poly time verifier for all 'yes' input $\}$

---

def Reduction :

Given two decision problem A & B, a reduction is a mapping from all instances I of A to I' of B s.t.

$$A(I) = YES \Leftrightarrow B(I') = YES$$

def poly time reduction.

Given two decision problems A and B, poly reduction is a poly time algo that maps an I of A to an I' of B s.t.

$$A(I) = YES \Leftrightarrow B(I') = YES.$$

We say $A \leq_p B$

598
Crypto

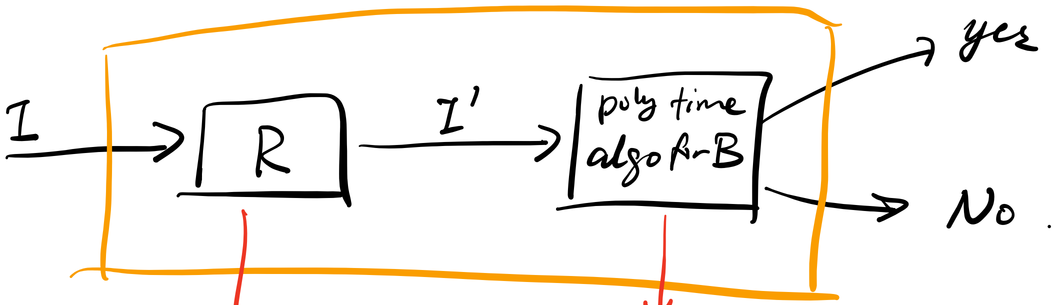
Claim Given $A \le_p B$, then a polytime B implies a polytime A.

Pf: Consider reduction R $\boxed{\text{from } A \text{ to } B}$

R in poly time $\Rightarrow$ $R_{AB}(|I|) \le poly(|I|)$

$\downarrow$

write at most $R_{AB}(|I|)$ bits $\Rightarrow$ $|I'| \le R_{AB}(|I|) \le poly(|I|)$



$$\underbrace{R_{AB}(I) \le poly(|I|) \qquad poly(|I'|) \le poly(|I|)}_{\text{poly time algo.}}$$

Reduction is transitive, $A \le_p B$, $B \le_p C \Rightarrow A \le_p C$

def NP hardness

a decision problem A is NP-hard if $\forall B \in NP$, $B \leq_p A$

def NP-completeness:

a decision problem A is NP-complete if:

(1) $A \in NP$

(2) A is NP-hard.

If A is NP-hard & $A \in P \Rightarrow P = NP$

Problem C is NP-hard, $B \leq_p C \leq_p A \Rightarrow B \leq_p A$ (transitivity)

Cook - Levin Theorem

SAT is NP- complete

3- SAT :

Given variables $x_1, \dots, x_n$

negation. optional.

$\downarrow$

clauses $C_1, \dots, C_m$, $C_i := (x_{\ell_1} \vee x_{\ell_2} \vee \neg x_{\ell_3})$

Find an assignment of $\{T, F\}$ to all $x_1, \dots, x_n$ s.t. all $C_1, \dots, C_m$ satisfied.

Thm 3SAT is NP- complete ($SAT \leq_p 3SAT$)

Pf: <u>Goal</u>: Find an algo that converts I of SAT to I' of 3SAT s.t.

I is satisfiable $\Leftrightarrow$ I' is satisfiable.

Idea: Replace OR , AND , NOT gates with clauses that has 3 vars.

$a = b \vee c \Rightarrow (\bar{a} \vee b \vee c) \wedge (a \vee \bar{b}) \wedge (a \vee \bar{c})$

$a = b \wedge c \Rightarrow (a \vee \bar{b} \vee \bar{c}) \wedge (\bar{a} \vee b) \wedge (\bar{a} \wedge c)$

$a = \bar{b} \Rightarrow (a \vee b) \wedge (\bar{a} \vee \bar{b})$

For clauses that has two vars. $(a \vee b) \Rightarrow (a \vee b \vee x) \wedge (a \vee b \vee \bar{x})$

one vars, ~~two dummy~~ vars.

Given a graph G w/ n vertices, m edges,

Q: $\exists$ a clique in G of size k? (K_k)

Claim: clique is NP-hard

SAT $\leq_p$ 3SAT $\leq_p$ CLIQUE

- For ever clause C, add variable (with negation if has) to the vertex set
- E connect all but complement (also not inside clause).

Claim: G has a clique of size m $\Leftrightarrow$ I has a satisfying assignment

$\Leftarrow$ For each clause, pick one literal that evaluates to true.

These literals selected forms a clique of size m.

⇒ If ∃ a clique of size m, . . .

Notice : all vertices of this clique comes from unique clauses.

⇒ m diffent clauses, ≡ m vertices

Pick vertex u associated w/ clause C

$$u \begin{cases} \to T & \text{if } u \text{ is in } C \\ \to F & \text{if } \bar{u} \text{ is in } C \end{cases} \Bigg\} \Rightarrow \begin{cases} \text{a valid assignment (no conflict).} \\ \text{a satisfying assignment (all true).} \end{cases}$$

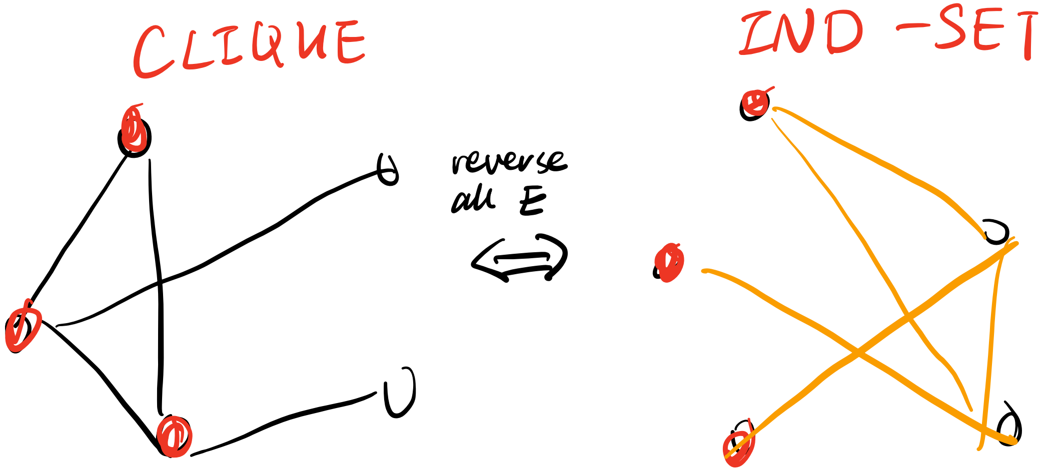
Independant Set Problem.

Given $G=(V,E)$, $|V|=n$, $|E|=m$, constant k, is there an independant set $S \subseteq V$ s.t $|S|=k$ and no two vertices is S share an edge.

This is NP since we have polytime verifier ⇒ we can certainly guess/construct the answer in poly time non-deterministically ?

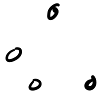
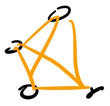
Show this is NP-hard : $\text{SAT} \le_p \le \underset{\uparrow}{\underline{\text{CLIQUE}}} \le_p \underset{\uparrow}{\underline{\text{IND-SET}}}$.

Example



So, idea is to construct $\bar{G} = (V, \bar{E})$.

Claim $\bar{G}$ has an independent set of size k ⟺ G has a clique of size k.

Pf: ⇒ Given ind-set  ⇒ 

⇐ Similar.

Vertex Cover Problem.

(1) Given $G=(V,E)$.

(2) $S\subseteq V$ is a vertex cover iff $\forall e=(u,v)\in E$, either $u\in S$ or $v\in S$.

Q $\exists$ S w/ $|S|=k$?

This is NP-hard : IND-SET $\leq_p$ Vertex Cover.

Claim : G has an independent set of size k

$\iff$ G has a vertex cover of size $n-k$.

$\equiv$ S is a vertex cover $\iff$ $V\setminus S$ is an ind-set.

Pf: $\Rightarrow$ Assume $V\setminus S$ is not an IS, then $\exists$ $u_0,v\in V\setminus S$ s.t. $(u_0,v)\in E$

But (u_0,v) is not in vertex cover. Contradiction.

$\Leftarrow$ Assume S is not a vertex cover, then

$$\begin{tikzcd}
\exists u,v\notin S, \arrow[d, Rightarrow] & \text{but } (u,v)\in E. \arrow[dd] \\
u,v\in V\setminus S \arrow[dr] & \\
 & V\setminus S \text{ not ind-set.}
\end{tikzcd}$$

Integer LP

$Ax \le b \qquad x \in \mathbb{R}^n$

x_i is integer $\forall i \in [n]$

Claim: ILP is NP-hard.

vertex-cover $\le_p$ ILP ?

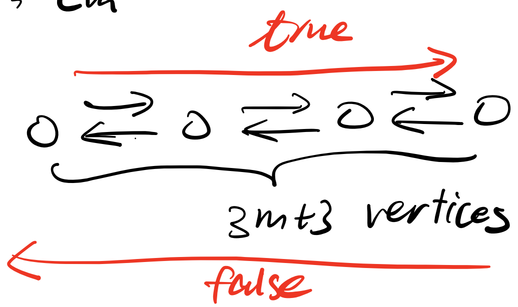
$\forall v \in G, \quad y_v = \begin{cases} 1 & \text{if } v \in S \\ 0 & \text{o.w.} \end{cases}$

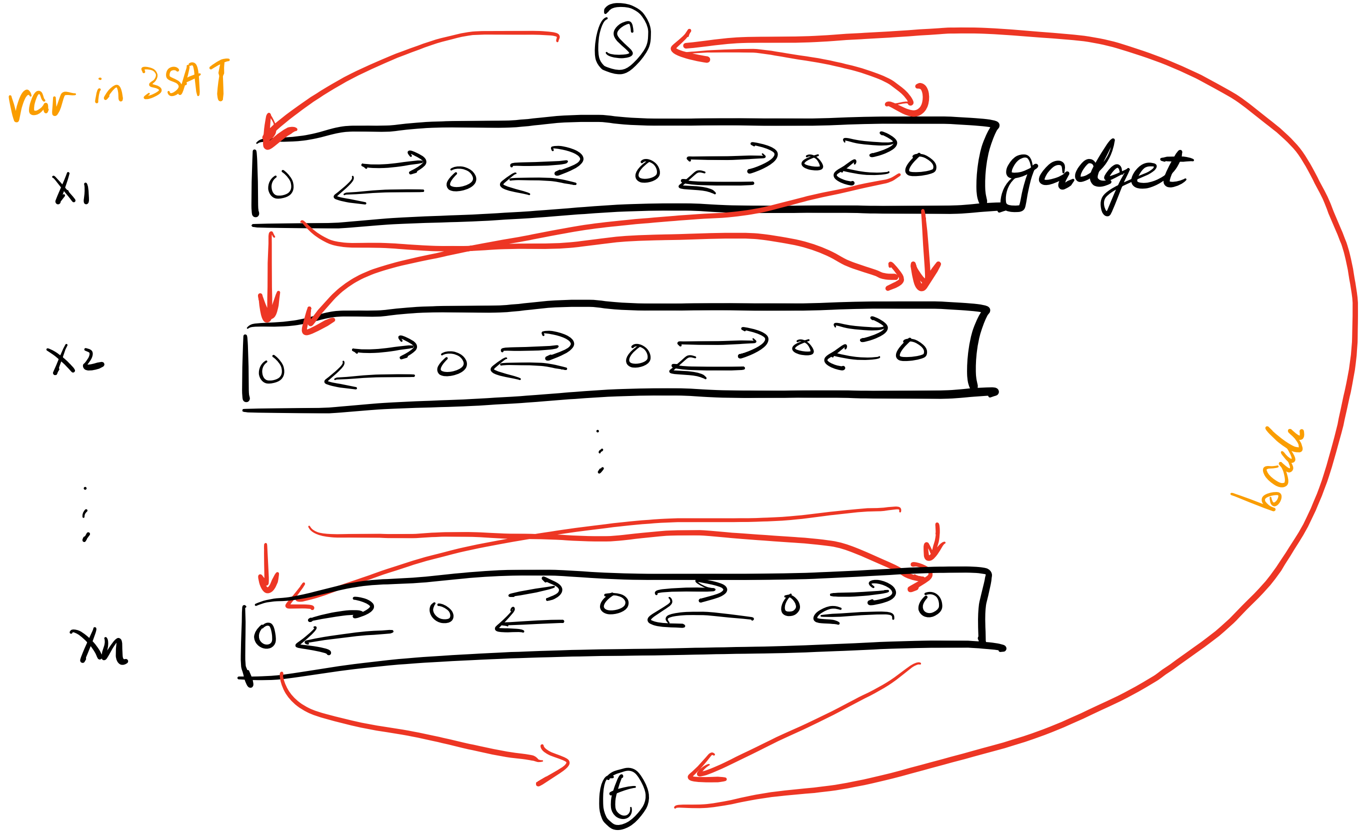
$$\left.\begin{array}{ll} \forall (u,v) \in E, & y_u + y_v \geq 1 \\ \forall v \in V & y_v \in \{0,1\} \\ & \sum_v y_v = k \end{array}\right\} \text{constraints.}$$

3SAT $\le_p$ Hamiltonian Cycle.

Given I : $\begin{cases} x_1, \dots, x_n \\ c_1, \dots, c_m \end{cases}$

$\forall x_i$, construct





exponential # of possible ham cycle.

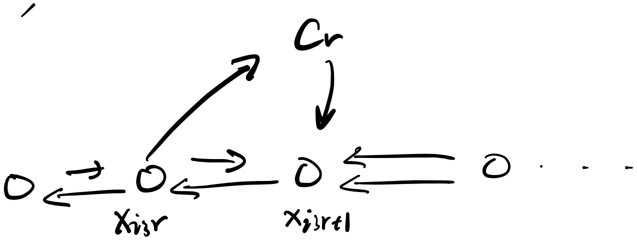
Structure : $S \to$ level 1 $\to$ level 2 $\to \dots \to$ level $n \to t$

Clause gadget : $C_i = (x \vee y \vee z)$

Introduce a new gadget : $C_r = (\underset{\{x_i, \neg x_i\} \cdots}{\underset{\cap}{l_i}} \vee l_j \vee l_k)$,

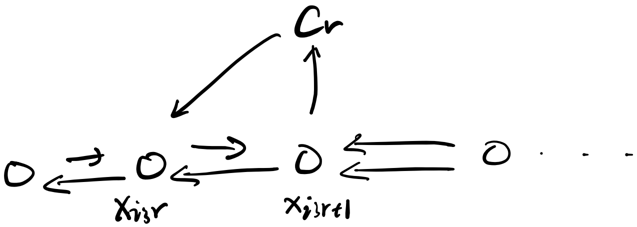
draw edges $x_{i3r} \to C_r \to x_{i3r+1}$

if $x_i = l_i$



$x_{i3r+1} \to C_r \to x_{j3r}$

if $\neg x_i = l_i$



Claim I of 3SAT has an assignment $\Leftrightarrow$ G has hamiltonian cycle.

3D matching

det Let X, Y, Z be finite sets